TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

NO PUBBLICITÀ 2,00 €
SOLO INFORMAZIONE E ARTICOLI

n.151

www.hackerjournal.it

HACKER JOURNAL

I RE DEI VIRUS

Viaggio nel più *GRANDE MERCATO* mondiale della *PIRATERIA*



ESCLUSIVA

INTERVISTA AD ALTROCONSUMO

su *PRIVACY* e *FILESHARING*

ANDROID

Alla *SCOPERTA* del *MISTERIOSO* "Gphone"

WI-MAX
Cosa è successo e cosa ci aspetta

LINUX

GUIDA ALLE PATCH del kernel by Andrew Morton

iPhone

ATTACCO AL FIRMWARE 2.0

Arriverà solo a *GIUGNO* ma è già in *PERICOLO*

hack·er (hãk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

Facciamo il **punto**

"I computer sono stupidi. Non sanno fare domande!"
Pablo Picasso (1881-1973)

Come avrete notato, alcuni anche con disappunto, da qualche mese in qua la nostra rivista ha subito dei cambiamenti, da parte nostra abbiamo cercato di fare in modo che non fossero traumatici per nessuno, da parte vostra ci avete premiato facendo in modo che la rivista sia sempre più acquistata e quindi abbia la forza di mantenere saldi quei principi con cui è nata:

- integrità morale
- spirito di divulgazione
- libertà di espressione
- distacco da ogni potere forte

Ci sembra che tutte queste premesse siano sempre rimaste le linee guida delle nostre pagine ma le domande si accalcano in continuazione su come possiamo ancora far evolvere la rivista, noi stessi e i nostri lettori ed ecco allora che decidiamo di dedicare un po' di spazio (mai troppo, promesso) a delle inchieste e a delle interviste che esulano un po' dal concetto di rivista tecnica.

Ripetiamo da tempo che l'hacking non è solo smanettare con codice e hardware ma è un vero e proprio "state of mind" e proprio in questa direzione abbiamo deciso di muoverci andando a scavare dentro alcuni aspetti della contro-cultura hacker cercando di approfondire più che le tecniche i concetti ed elevare così lo stato delle nostre intelligenze da pratiche a teoriche per poterne tornare alla fase pragmatica ancora più forti, tutelati e consapevoli di prima.

Speriamo, ed io in particolar modo, che tutto questo abbia come sempre un favorevole riscontro presso di voi e che questa nostra nuova sfida giornalistica venga accolta con l'entusiasmo che merita, sempre e comunque pronti a ricrederci e a cercare nuove strade.

Buona Lettura

The Guilty

CONTINUA LA CACCIA

In tanti ci hanno già risposto ma non ci basta mai e vogliamo solo il meglio per le nostre pagine e i nostri lettori e quindi continuate a mandare le vostre candidature alla mail:

contributors@hackerjournal.it

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Anno 8 – N.151
15 / 28 Maggio 2008

Editore (sede legale):
WLF Publishing S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

Nuovo schiavismo e Infezioni

Quando si parla di sfruttamento del lavoro si pensa sempre ai bambini cinesi che cuciono palloni o scarpe per qualche multinazionale dello sportswear, in realtà ormai esiste un fiorente mercato dello sfruttamento anche nel mondo dell'informatica e in particolar modo della pirateria. Il problema che gli spammer si trovano a dover affrontare sempre più di frequente è lo scavalcamento dei CAPTCHA che riescono normalmente a bloccare il 70% dei tentativi effettuati da botnet, il problema è stato risolto istituendo delle vere e proprie factory in paesi in via di sviluppo dove, per pochi euro al giorno, migliaia di nuovi schiavi inseriscono dati tutto il giorno inserendo codici CAPTCHA per conto di spammer professionali.



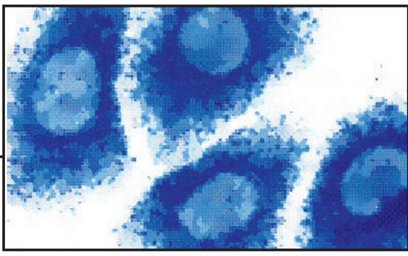


Era già successo in occasione dei mondiali di Rugby in Francia e ora la storia si ripete per i campionati europei di calcio, attenzione agli acquisti di biglietti tramite la rete. Questo a seguito dell'individuazione di un malware noto come Mal/ObfJS-R sul sito web di un importante rivenditore di biglietti.

Il sito in questione vanta un ottimo posizionamento nei motori di ricerca e una presenza costante tra i link sponsorizzati, quindi gli hacker potrebbero avere a disposizione un alto numero di potenziali vittime.

Mezzo milione di siti colpiti da Sql Injection a causa di Microsoft IIS e Microsoft Sql Server, Redmond continua a dire che la colpa non è dei suoi software ma del mancato rispetto delle procedure di sicurezza da parte degli amministratori dei database ma fatto sta che i pirati hanno utilizzato proprio una caratteristica di IIS per effettua gli attacchi. Il sistema permette infatti l'uso di comandi generici che non richiedono argomenti specifici a livello di tabella.

© 2004 UEFA TM
UEFA
EURO2008
Austria-Switzerland



1 MILIONE DI VIRUS

Queste cifre apocalittiche vanno sempre prese con le pinze, soprattutto quando vengono comunicate da chi vende soluzioni antivirali, ma il dato è comunque interessante. Symantec ha pubblicato un rapporto sulla sicurezza della Rete, nel quale il conteggio dei virus, worm e trojan horse circolanti supera per la prima volta il milione.

Il dato più significativo è che la stragrande maggioranza di questi malware (programmi ostili) è recente: quasi i due terzi sono stati creati negli ultimi dodici mesi. E il 2007 mostra una tendenza di crescita impressionante: la seconda metà dell'anno, infatti, ha visto un aumento del 136% nei nuovi malware rispetto ai primi sei mesi. Che siano davvero nativi, come in molti pensano, delle stesse case costruittrici di antivirus?

IBM SEMPRE PIÙ PICCOLO

Questa settimana IBM ha annunciato di essere pronta a fabbricare prototipi di chip costruiti con una tecnologia di processo a 32 nanometri. Big Blue sta sviluppando tale tecnologia all'interno di un'alleanza di cui fanno parte Chartered, Infineon, Samsung, Sony, Toshiba, Freescale e STMicroelectronics.

La commercializzazione dei primi processori a 32 nm è attesa per il 2010. La nuova tecnologia a cui lavorano IBM e soci si fonda su quello che gli esperti chiamano processo high-k gate-first. L'azienda di Armonk afferma che i chip high-k/metal gate riusciranno a consumere circa il 45% di energia in meno e potranno incrementere le performance di circa il 30%, inoltre saranno compatibili con un'ampia gamma di applicazioni: dai microchip a basso consumo destinati ai dispositivi wireless o ad altri dispositivi consumer ai microprocessori ad alte prestazioni destinati ai computer aziendali o alle console da gioco.

NAVIGARE NELL'ACQUA

Il futuro della connettività è oggi giorno ancora rallentato dalle bariere delle vecchie infrastrutture. Sostituire, gli ormai obsoleti fili di rame, è impensabile e soprattutto molto costoso. Per questo la Ofcom, e i suoi ingegnieri inglesi stanno studiando un nuovo sistema per oviare il problema facendo passare la fibra ottica nelle attuali condutture idriche e fognarie. Le condutture di trasporto dell'acqua e i punti di accesso sotterranei alla rete potrebbero celare ampio spazio per la posa veloce ed economica di infrastrutture di connettività, esattamente come accade in molte aree di diversi paesi, Italia compresa, dove la fibra viene fatta correre dentro, sopra, sotto e accanto le reti delle utility.



Quindi, probabilmente, il futuro della navigabilità sono le acque delle nostre città.

UBUNTU 8.04

Dopo quattro anni, dal rilascio di GNU/Linux, è arrivato in contemporanea mondiale Ubuntu 8.04 (per gli amici Hardy Heron). Il nuovo sistema operativo basato su Linux che promette di portare la rivoluzione del software libero in tutti i computer.

La cosa che rente davvero questo software completo è la sua comunità internazionale, organizzata in quattro divisioni fondamentali: sviluppo,

A caccia del FIRMWARE 2.0



Abbiamo scatenato i nostri segugi e trovato il nuovo firmware, in uscita a giugno, per il gioiellino telefonico di casa Apple

Dal 9 al 13 giugno prossimo si svolgerà a San Francisco il Worldwide Developers Conference (WWDC), attesissimo appuntamento annuale fissato dalla Apple per presentare tutte le novità dei suoi prodotti all'interno del quale è prevista una sessione specifica dedicata all'iPhone e alla nuova versione del suo sistema operativo.

Ma per gli sviluppatori e pochi fortunati è già disponibile la beta (early beta) del nuovo firmware che probabilmente sarà rilasciato come versione 2.0 di iPhone. Il condizionale è d'obbligo perché non è detto che la Apple cambi idea poi e introduca delle versioni intermedie, tipo 1.1.5 o 1.2.

Per chi le ha potute vedere da vicino, le funzionalità che verranno introdotte sono molto interessanti soprattutto perché si migliorano le caratteristiche multimediali proprie di iPhone e perché si strizza l'occhio al settore business, un ambito in cui sembra regnare incontrastato il Blackberry della Research In Motion (RIM).



Apple ha infatti aquistato e integrato nel prossimo firmware la licenza per ActiveSync di Microsoft che permette all'iPhone la sincronizzazione dei dati con Microsoft Exchange Server (standard di fatto per molte realtà aziendali) 2003 e 2007. Con questa caratteristica, sarà possibile leggere la posta aziendale e gestire gli appuntamenti, le scadenze, le pianificazioni, come se si fosse fisicamente in ufficio. Chiaramente per proteggere le connessioni tra il proprio iPhone e il server aziendale deve essere realizzata una connessione sicura su un canale criptato e una tecnologia matura per questo tipo di servizio è la Virtual Private Network (VPN). Nelle immagini presenti in rete, tra le opzioni presenti nella configurazione del firmware 2.0 delle VPN a bordo dell'iPhone compare anche il logo della VPN IPSec di Cisco, il gigante degli apparati di rete che fanno funzionare internet. Una partnership questa che è una sicura garanzia per la professionalità richiesta in una connessione protetta. E pare che la stessa Microsoft non sia assolutamente indifferente al successo che sta riscuotendo il gioiellino della Apple. Proprio in questi giorni Tom Gibbons, il vice presidente della divisione di Microsoft dedicata ai dispositivi e applicazioni, in un'intervista rilasciata a Fortune lascia intendere che stanno studiando da vicino il mercato che gravita intorno all'iPhone in modo da proporre quanto prima porting dei loro prodotti (e si vocifera che una versione di Microsoft Office per iPhone sia già in cantiere). E' possibile quindi che già da giugno sia rilasciata qualche applicazione per iPhone definita Office-ready, che permetta quindi di leggere i comuni formati Word ed Excel senza poterli però editare.
Evidentemente iPhone ha portato grandi novità in un mercato finora dominato da dispositivi con WindowsCE, Symbian e Blackberry, quindi probabilmente la Microsoft vuole anticipare possibili concorrenti cercando di imporre i suoi prodotti software su una piattaforma promettente, dove (ancora) il suo monopolio non è arrivato.





Un'altra interessante novità (attesa sempre a partire da giugno), sarà la possibilità di installare software di terze parti acquistandole direttamente dal proprio iPhone tramite iTunes App Store, il negozio online della Apple (nella nuova interfaccia del nuovo firmware compare un tasto dedicato App Store).

L'idea di Apple è semplice: è stato rilasciato un Software Developer Kit completamente gratuito per sviluppare software sia per iPhone che per iPod, ma pagando 99 dollari si può rivendere il proprio software tramite il negozio ufficiale della Apple.
Nel costo di iscrizione è compreso il supporto tecnico e tutta la documentazione a corredo di Apple.

Lo sviluppatore poi decide il prezzo di vendita ricevendo il 70% dell'incasso su base mensile, mentre il resto va chiaramente alla Apple. Per le applicazioni freeware ci sarà invece spazio completamente gratuito. In pratica viene stimolata la produzione di software, professionale o amatoriale che sia, dando la possibilità di ricevere una sponsorizzazione di primo piano proprio dal produttore di iPhone e iPod a un costo decisamente abbordabile (soprattutto per noi europei con il cambio a nostro favore).
Si prevede che durante il WWDC venga presentato ufficialmente il negozio online e che verranno quindi mostrate tutte le possibilità offerte agli sviluppatori e agli esperti IT.
Ma vediamo quali dovrebbero essere le altre funzionalità introdotte che



CRACK 1.0

Qualcuno ricorderà il clamore generato dal crack della protezione dei DVD (chiamato DeCSS) pochissimo tempo dopo l'accordo raggiunto tra i vari produttori mondiali sullo standard definitivo da adottare per distribuire e vendere i film. L'autore del crack, Jon Lech Johansen, è stato ribattezzato da allora come DVD Jon ed è lo stesso autore della sprotezione (o come si dice in rete, liberazione) dell'iPhone. Grazie all'ingegno di questo ragazzo norvegese, l'iPhone che sarebbe vincolato a funzionare con le sole sim del gestore telefonico americano AT&T, può invece funzionare con qualunque sim, incluse quelle italiane. Ci sono diversi tutorial in rete che arrivano fino alla versione 1.1.4 e che spiegano passo passo come liberare l'iPhone.

sono state già anticipate o sono state carpite leggendo le stringhe presenti nel firmware:

- la ricerca tra i contatti non si attiva da subito, ma solo quando il numero dei contatti salvati diventa elevato (è comparsa la lente Spotlight);
- nell'applicazione Calendario è presente un nuovo pulsante che ancora non è attivo così come non è ancora attivo il pulsante per collegarsi all'App Store;
- il Parental Control, che permette di limitare i contenuti fruibili dai minori, è perfettamente funzionante;
- è possibile riordinare le reti Wi-Fi in base alle proprie preferenze; è stata poi inserita l'applicazione Bonjour (già nota agli utenti Mac) che permette di connettere in modo semplificato tra loro più dispositivi nella stessa rete Wi-Fi (e a detta di molti che già lo usano sembra sia insostituibile);
- la Calcolatrice è stata modificata in modo molto interessante: se si lancia l'applicazione quando l'iPhone è in posizione verticale parte l'applicazione standard, mentre se l'applicazione è in funzione e si ruota l'iPhone in orizzontale si passa alla modalità scientifica; inoltre i tasti sono stati ridisegnati da rotondi a quadrati;
- è finalmente possibile effettuare selezioni multiple dei messaggi nell'applicazione Mail per eliminarli, copiarli o spostarli in un colpo solo senza doverlo fare per un messaggio alla volta;
- è possibile andare nella modalità a schermo intero, sia per il browser Safari che per le singole applicazioni e Safari supporterà finalmente i video di YouTube (ancora non è chiaro se con un plugin realizzato appositamente o come supporto nativo del browser);
- sono state integrate le tecnologie di grafica vettoriale scalare (SVG) che permettono di fruire di immagini di qualità elevata ad un peso in byte molto inferiore e sono stati introdotti nuovi effetti CSS;
- ci sarà il supporto per le presentazioni in PowerPoint (nel formato pps);
- sembra che con la versione 2.0 ci sarà il supporto del costoso servizio .Mac di Apple che permette di integrare posta elettronica, backup dei documenti del Mac, la crezione di gallerie fotografiche online, hard disk virtuali e altro; infatti da un'analisi sulle stringhe presenti nel firmware si legge "*Syncing with this Dot Mac account will turn off syncing for other Dot Mac accounts and delete any existing synced data*".



Oltre a queste succulente novità (per le quali comunque si dovrà aspettare il lancio ufficiale dato che compaiono solo negli screenshot presenti nell'SDK e nelle presentazioni della Apple), ci sono indiscrezioni piuttosto serie sulla possibilità che insieme al lancio del nuovo firmware venga presentata una nuova versione dell'iPhone che supporti le reti 3G (UMTS). Per la verità, questa voce gira da parecchio tempo in rete, ma Ken Dulaney, un analista della Gartner, ha dichiarato negli ultimi giorni che la Apple ha ordinato 10 milioni di terminali 3G e si parla anche della presenza della tecnologia OLED (la stessa inaugurata in alcuni degli ultimi cellulari SonyEricsson e Motorola) per realizzare forse un iPhone più sottile. Se queste notizie venissero confermate, ci sarebbe sicuramente una reazione decisamente più vivace, non solo oltreoceano dove gli iPhone vengono venduti da tempo (anche se ufficialmente bloccati sulla rete di AT&T, vedi box), ma anche nel mercato europeo rispetto a quanto è avvenuto e sta avvenendo per la versione attuale dell'iPhone (fuori USA reperibile quasi esclusivamente tramite ebay). L'Europa infatti si è lanciata da tempo nelle connessioni a banda larga tramite reti mobili (da noi già si parla di 3,5G e 4G) e molti hanno considerato un grave handicap la mancanza di questa connettività sull'iPhone. Dalle indiscrezioni sembra poi che ci sarebbero tre varianti di iPhone 3G: una da 8GB (a 399 dollari), una da 16GB (a 499 dollari) e una con la bellezza di 32GB (a 599 dollari). Praticamente uno smartphone e un hard-disk portatili da usare anche per scaricare contenuti multimediali a banda larga, con l'appeal di Apple.
Si parla di indiscrezioni perché la Apple non ha rilasciato alcun comunicato in merito. Occhi puntati quindi sul prossimo appuntamento del WWDC e come si dice in questi casi, stay tuned!

CRACK 2.0 - BETA -

Non è ancora uscito il firmware 2.0, ma il DevTeam ha già dimostrato come si possano aggirare le protezioni inserite da Apple per far girare sull'iPhone applicazioni di terze parti non certificate dalla stessa Apple. In pratica il team ha realizzato una versione modificata del codice di boot del telefono che permette di intercettare il controllo dell'iPhone prima che lo faccia il sistema operativo. Questa possibilità apre molti scenari, tra cui chiaramente la libera sperimentazione. Il progetto si chiama Pwnage ed è stata appena rilasciata la versione 1.1 che supporta l'ultima build rilasciata del firmware per iPhone (5A240d); inoltre nel loro sito sono disponibili liberamente i codici modificati. Tra l'altro il loro tool chiude anche un bug del firmware di Apple relativo alla gestione WiFi.

A caccia di privacy con IdentiFight

Un motore di ricerca che scandaglia Internet per controllare se un nostro indirizzo è pubblico (e quanto) e suggerisce come intervenire per aumentare il livello di privacy

L'idea è venuta allo sviluppatore Alf Eaton giocando con Spokeo, un super-aggregatore di blog, foto, e video assemblati da social network e feed vari: Eaton è rimasto colpito di quanto spesso le email degli utenti dei vari siti e servizi fossero in bella vista ed ha deciso di fornire un piccolo quanto utile strumento per essere più consapevoli della propria identificabilità su Internet.



:: Chi cerca trova

Il risultato si chiama IdentiFight (http://identifight.org/) e, datogli in pasto un indirizzo e-mail, ricercherà quanti più siti possibili con profili alla ricerca dell'indirizzo di posta. I risultati non sono solo una lista di sterili avvertimenti ma contengono, quando possibile, voce per voce anche dettagli su come intervenire per modificare la visibilità delle informazioni personali in alcuni casi con la procedura passo passo nelle impostazioni del servizio.



IdentiFight riesce a indagare ed interagire con siti noti e molto usati come Flickr, Friendster, LiveJournal, Magnolia, Rapleaf, Spock, StumbleUpon, Vox, Yahoo! 360°e Yelp ma fornisce comunque informazioni e link utili su come viene gestita la privacy degli utenti in una ventina di siti (http://identifight.org/browse) tra cui troviamo Amazon.com, Pownce, Twitter, Last.fm, LinkedIn o Twitter.

:: Come funziona

L'indirizzo inserito viene sottoposto da IdentiFight al search form (o alle API, nel caso di Flickr) di più siti. Questa operazione viene fatta in contemporanea usando curl_multi_exec, una funzione della libreria libcurl in PHP.

Se il sito lo richiede il motore fa login per poter ricercare l'indirizzo e-mail e poi, nelle pagine di risultati, fa lo scraping di nome, username, foto, un link e l'estratto del profilo. Tutti i link ai profili vengono poi sottoposti alle API Social Graph di Google che fornisce eventuali altri indirizzi connessi per mezzo del microformato rel="me". Da questi risultati vengono selezionati i nomi e le username più usate che saranno chiavi ulteriori di ricerca su altri siti (come Google). A questo punto il risultato viene sottoposto all'utente.

:: I limiti

Identifight è uno strumento di ricerca e di informazione: i suoi limiti ultimi derivano da quanto concedono Yahoo! e gli altri provider. Se un servizio non permette a client esterni di accedere ai profili personali (o lo rende tecnicamente complicato) Identifight non può garantire nulla, come nel caso di Facebook o di MySpace. Peggio ancora può succedere che i siti non contemplino il rimuovere o quantomeno nascondere i dati e, anche quando si chiude l' account e si termina la fornitura del servizio, le informazioni personali rimangano al loro posto.

Nicola D'Agostino
www.nicoladagostino.net

Inside Android

Alla scoperta dell'attesissimo sistema opertativo per smartphone made in Google



Lo scorso novembre Google ha annunciato nello stesso giorno il rilascio di Android e la nascita della Open Handset Alliance (OHA), un accordo che riunisce al momento circa 34 diverse aziende dei semiconduttori, dell'elettronica, della telefonia mobile, del software ed altri, con lo scopo di definire e promuovere uno standard aperto comune per i dispositivi mobili, sotto il suo coordinamento. Oltre Google, tra le aziende più importanti figurano HTC, Intel, Motorola, Qualcomm, T-Mobile, NVIDEA, LG, Samsung, Texas Instruments e la nostra Telecom Italia. Non è un caso che Microsoft non ne faccia parte quindi!



Android è una piattaforma di sviluppo software per dispositivi mobili che include un sistema operativo basato sul kernel 2.6 di linux, il middleware (ossia tutti quei tool necessari agli sviluppatori software per elaborare il codice tra applicazioni differenti) e delle applicazioni di base. Il linguaggio scelto per lo sviluppo è Java, quindi è l'unico supportato al momento.



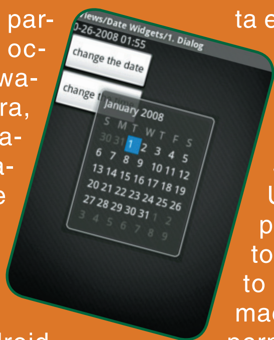
Si parla chiaramente di un kit di sviluppo (Android SDK) comprensivo di tutta la documentazione necessaria per avere su un dispositivo complesso come può essere un telefonino, un ambiente operativo completamente aperto e personalizzabile che permetta di sviluppare rapidamente le proprie applicazioni.

All'interno di Android troviamo una gestione a framework, ossia con la possibilità di sostituire le singole componenti, una macchina virtuale ottimizzata per dispositivi mobili chiamata Dalvik, un browser integrato basato su WebKit (sempre open source), librerie grafiche 2D e 3D basate su OpenGL ES 1.0, supporto dei comuni formati audio e video (MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, GIF) , il piccolissimo ed efficiente motore database SQLite

(occupa appena 500kb), un emulatore, strumenti di debug, ottimizzazione e profiling e un plugin per utilizzare Eclipse come ambiente di sviluppo. Oltre alla dotazione propriamente software, in base all'hardware che vogliamo gestire, c'è il supporto per la telefonia GSM (EDGE/3G), i collegamenti Bluetooth e WiFi, la fotocamera, il gps, la bussola, l'accelerometro.

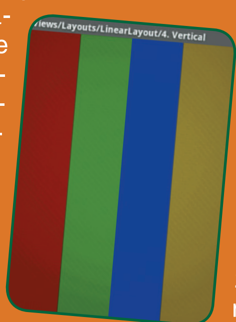


L'architettura di Android può essere visualizzata a strati. Si parte dal kernel (linux) che si occupa di gestire tutto l'hardware di basso livello (fotocamera, bluetooth, memorie flash, tastiera, wifi, audio, power management, comunicazione tra kernel e software), al di sopra del quale viene fornita un'ampia quantità di librerie di gestione, comprese quelle proprie di Android e Dalvik, che fungono da interfaccia allo sviluppatore. Al di sopra delle librerie infatti, è possibile selezionare nell'Application Framework cosa si andrà a rilasciare sul dispositivo, scegliendo tra diversi gestori indipendenti (Activity Manager, Window Manager, Content Providers, View System, Package Manager, Telephony Manager, Resource Manager, Location Manager, XMPP Service) per definire esattamente che tipo di dispositivo stiamo realizzando.





Ad esempio, l'Activity manager gestisce il ciclo di vita di un'applicazione e fornisce la navigazione da e verso questo applicazione; il Content Provider si occupa di permettere alle applicazioni di accedere ai dati di altre applicazioni (ad esempio i contatti) per condividerli; il Resource Manager fornisce l'accesso alle risorse non direttamente legate al codice (come le stringe di localizzazione, i grafici, i file di layout); il Notification Manager permette a tutte le applicazioni di notificare allarmi sulla status bar.



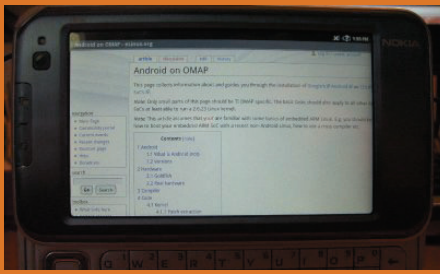
Inoltre, tra le funzionalità di base del dispositivo gestito da Android già disponibili ci sono un client e-mail, un programma di gestione sms, il calendario, le mappe, il browser, i contatti ed altre, tutto scritto in Java. Anche gli esempi forniti con l'SDK sono scritti in Java e sono già pronti da usare, come il DatePicker e il TimePicker, che permettono all'utente di selezionare data e ora graficamente, la Gallery per vedere la preview delle foto scattate con la fotocamera e selezionarle poi con ImageSwitcher.

Una volta realizzata il proprio software va verificato il corretto funzionamento e per i test si utilizza la macchina virtuale Dalvik che permette di lanciare ogni singola applicazione in un processo separato. Dalvik permette anche di lanciare diverse virtual machine e basa tutto ciò che riguarda la sicurezza, la gestione della memoria e dei processi, lo stack network e la gestione dei driver sulla versione 2.6 del kernel Linux, beneficiando quindi di tutte le caratteristiche introdotte recentemente.

Per promuovere lo sviluppo di una comunità intorno ad Android, Google ha lanciato una sfida in perfetto stile americano: 10 milioni di dollari per premiare le 50 migliori applicazioni realizzate con (e per) Android da inviare al sito dedicato ad Android entro lo scorso 14 aprile. Tra i suggerimenti dati, si consigliava di realizzare applicazioni di social networking, fruizione e gestione di contenuti multimediali o produttività e collaborazione (come e-mail, calendari, programmi di messaggistica), giochi, gestione di notizie e informazioni, applicazioni di mash-up ossia di rielaborazione delle informazioni a partire da diverse fonti, utilizzo del GPS per servizi di localizzazione, ripensamento di interfacce classiche, applicazioni per scopi umanitari e sviluppo di servizi per l'economia globale.



In questo momento Google sta testando ognuna delle applicazioni pervenute allo scopo di redigere una classifica generale entro il prossimo 5 maggio e premiare le migliori 50 applicazioni con 25 mila dollari ciascuna.



Questi fondi verranno erogati al fine di continuare lo sviluppo e partecipare a una seconda selezione che dovrà selezionare tra queste 50 le migliori 20. Le prime 10 riceveranno ben 275 mila dollari, le altre 100 mila dollari. Purtoppo per questioni fiscali, soltanto i residenti in USA potevano partecipare a questa gara. Al momento Android è stato pensato per funzionare solo su Windows, Linux (x86) e MacOS X (Intel), ma sono stati già effettuati dei porting non ufficiali su altre architetture. La stessa STMicroelectronics ha mostrato un prototipo del suo processore Nomadik che funziona con una versione di Android rielaborata da Wind River System e in rete si trovano informazioni relative al funzionamento di Android sull'Internet Table N810 di Nokia funzionante con Android (nonostante la Nokia non faccia parte della OHA). Quanto mancherà all'uscita del primo Gphone? ■

Alla fine dei conti

La gara si è finalmente chiusa e vediamo di capire cosa succederà di questa presunta rivoluzione...



Il WiMAX (Worldwide Interoperability for Microwave Access) è uno standard mondiale che consente l'accesso a reti di telecomunicazioni a banda larga e senza fili e come suggerisce il nome deriva dal noto WiFi. Ma sono molte le differenze, in particolare con il WiMAX c'è la possibilità di raggiungere una banda di circa 70Mbit/s in area metropolitana con una copertura fino a qualche chilometro (nominalmente si dovrebbe arrivare a 50Km) per mezzo di una singola stazione base erogando una potenza massima di 4 Watt.
Altre caratteristiche interessanti riguardano la possibilità di supportare non solo una connessione punto-punto, ma anche connessioni punto-multipunto (MESH), l'implementazione di diverse tecniche di crittografia, sicurezza e autenticazione contro intrusioni, ben cinque diversi tipi di gestione della qualità del servizio (QoS) ed è possibile utilizzare un'antenna ricevente in mobilità fino alla velocità di 160Km/h. Quindi sarebbe possibile dotare un'automobile di antenna WiMAX per assicurare un collegamento a banda larga anche a velocità di crociera in autostrada installando stazioni ripetitrici lungo il percorso e telefonare con un client VoIP (Skype ad esempio) mentre siamo in viaggio.



Nelle speranze dei promotori, c'è la possibilità di poter raggiungere tutto il territorio con un collegamento superveloce, anche le aree morfologicamente più disagiate e quindi non raggiunte dall'ADSL (o UMTS) e chiaramente promuovere una maggior competizione nel mercato. E il vantaggio rispetto alle reti mobili è davvero notevole: tanto per quantificare, il WiMAX offre a metà costo una velocità di trasmissione dati tre volte superiore a quella offerta dai network su cui lavorano i cellulari, per cui si ipotizza che il WiMAX potrebbe persino sostituire l'UMTS. Letteralmente un terremoto per i gestori telefonici mondiali. Sarà un caso che esistono pochi terminali sul mercato che supportano sia l'UMTS che il WiFi?
A regime si vorrebbe riuscire ad abbattere il cosiddetto digital-divide, permettendo a tutti i cittadini di beneficiare di un collegamento continuo e a banda larga a costi ridottissimi, così come avviene in altri stati europei già da tempo. Si stima infatti che siano oltre 4 milioni i cittadini italiani esclusi in questo momento e contrariamente a quanto si possa pensare per la maggior parte sono concetrati nel centro-nord Italia (circa 2,6 milioni). E ci sono cir-

raggiunti da collegamento ADSL hanno comunque un limite di banda di 640 kbit/s (ADSL lite).
La ragione del ritardo dell'Italia è dovuta alla richiesta dello standard di utilizzare le frequenze comprese tra i 3,4-3,6GHz che precedentemente erano assegnate al Ministero della Difesa. È stato necessario quindi attendere che venissero liberate prima di poter procedere alla riassegnazione.
Come in Francia, anche in Italia è stato deciso di licenziare tali frequenze ed è stata indetta un'asta che si è conclusa lo scorso febbraio. L'Italia è stata suddivisa in macro-aree, per ognuna delle quali erano disponibili tre concessioni. Tra i soggetti aggiudicatari ci sono sì nomi noti (Telecom Italia per dirne uno), ma sono comparse realtà aziendali decisamente meno conosciute che probabilmente faranno parlare di sé molto presto. Un nome tra tutti è ARIADSL, un piccolo provider umbro che finanziato da un privato di origini israeliane è riuscito ad aggiudicarsi l'assegnazione di frequenze per ogni macrozona d'Italia. Iniziano a trovarsi in commercio i primi dispositivi WiMAX, ma anche in questo caso nessun cellulare.

È possibile che si configuri un conflitto diretto tra dispositivi propriamente mobili e nuovi dispositivi wireless. Sarà come sempre il mercato a stabilire come andranno le cose, anche se è possibile che per servizi di emergenza o comunque prettamente vocali siano i cellulari a vincere la competizione, perché già padroni del mercato. Mentre nel lungo periodo, con una maggiore fruibilità di internet, nuovi dispositivi ibridi consentano a un pubblico più smaliziato ed esigente di utilizzare maggiori applicazioni in situazioni che ora non si riescono nemmeno a prevedere.



Aggiudicatari dei 7 diritti d'uso nazionali - Blocco A
Area di gara Regioni rappresentate
1 Lombardia-Bolzano-Trento => ARIADSL
2 Valle d'Aosta-Piemonte-Liguria-Toscana => ARIADSL
3 Friuli Venezia Giulia-Veneto-Emilia Romagna-Marche => ARIADSL
4 Umbria-Lazio-Abruzzo-Molise => ARIADSL
5 Campania-Puglia-Basilicata-Calabria => ARIADSL
6 Sicilia => A.F.T.
7 Sardegna => ARIADSL



Aggiudicatari dei 7 diritti d'uso nazionali - Blocco B
Area di gara Regioni rappresentate
1 Lombardia-Bolzano-Trento => E-VIA GRUPPO RETELIT
2 Valle d'Aosta-Piemonte-Liguria-Toscana => E-VIA GRUPPO RETELIT
3 Friuli Venezia Giulia-Veneto-Emilia Romagna-Marche => E-VIA GRUPPO RETELIT
4 Umbria-Lazio-Abruzzo-Molise => Telecom Italia
5 Campania-Puglia-Basilicata-Calabria => Telecom Italia
6 Sicilia => Tourist Ferry Boat-Temix-Medianet Comunicazioni
7 Sardegna => Telecom Italia



Aggiudicatari dei 21 diritti d'uso regionali - Blocco C
Area di gara Regioni rappresentate
1 Lombardia => A.F.T.
1 Prov. Aut. Bolzano => Brennercom
1 Prov. Aut. Trento => MGM Productions Profit Group
2 Valle d'Aosta => Ribes Informatica-Hal Service-Lan Service-Informatica System-Tex97-B.B.Bell
2 Piemonte => A.F.T.
2 Liguria => MGM Productions Profit Group
2 Toscana => MGM Productions Profit Group
3 Friuli Venezia Giulia => Assomax
3 Veneto => A.F.T.
3 Emilia Romagna => Infracom
3 Marche => City Carrier
4 Umbria => A.F.T.
4 Lazio => A.F.T.
4 Abruzzo => A.F.T.
4 Molise => A.F.T.
5 Campania => A.F.T.
5 Puglia => A.F.T.
5 Basilicata => A.F.T.
5 Calabria => A.F.T.
6 Sicilia => ARIADSL
7 Sardegna => A.F.T.

I DATI DELL'ASTA



L'ELDORADO dei pirati

Una ricerca di Panda Security conferma il "momento nero" dei software antivirus. Ecco perché non siamo più al sicuro

Un computer su quattro, anche se è protetto da un programma antivirus, è infetto. Nelle reti aziendali, invece, la proporzione è addirittura di tre LAN infette su quattro. I dati arrivano da una ricerca effettuata da Panda Security e mette in luce un fenomeno che molti specialisti di sicurezza avevano già denunciato da tempo: di fronte ai continui assalti dei virus informatici, i software per la sicurezza stanno perdendo colpi.

:: Una nuova era

I tempi sono cambiati e con essi il tipo di minacce che si annidano sul Web. Se fino a qualche anno fa la figura del pirata informatico era identificata con la romantica figura del "genio incompreso" che cercava una rivincita nei confronti dell'azienda che lo aveva maltrattato o agiva con il semplice scopo di ottenere fama e prestigio, oggi chi scrive virus informatici ha un solo scopo: guadagnare denaro.

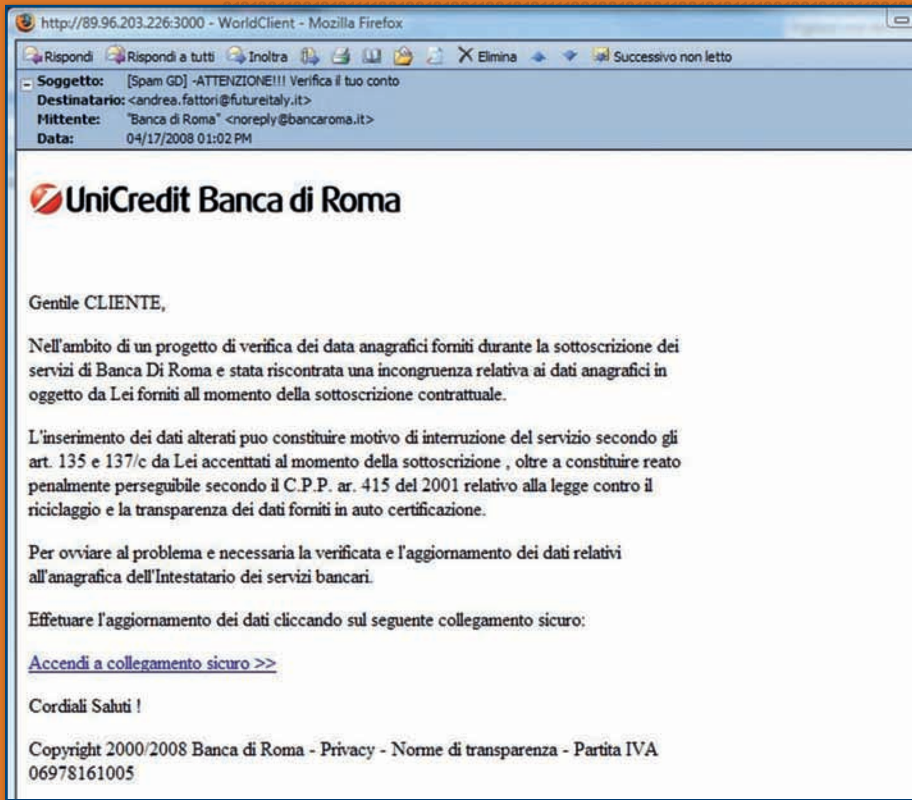
A provocare questa trasformazione è stato lo sviluppo di Internet e l'uso massiccio di carte di credito sul Web, che rappresentano un boccone estremamente ghiotto per chi ha le conoscenze per creare e diffondere virus. Secondo i dati diffusi da Panda Security, il XX% dei virus identificati nel 2007 erano trojan, ovvero virus che hanno lo scopo specifico di consentire il controllo a distanza del computer infetto.

Una funzione spesso utilizzata per rubare informazioni riservate.

:: Gang criminali

Nella vicenda, però, non sono quasi mai coinvolte singole persone. Il mercato dei virus coinvolge infatti vere "gang" criminali che si muovono nei bassifondi di Internet per realizzare i loro guadagni. Chi vuole guadagnare con il crimine informatico, oggi, non ha nemmeno bisogno di conoscenze informatiche particolarmente approfondite: bastano i contatti giusti. Sul Web, infatti, è possibile comprare un virus nuovo di zecca per poi diffonderlo. Lo scopo è quello di infettare il maggior numero di PC per

ottenere una botnet, ovvero una rete di computer controllabili a distanza, pronti a eseguire qualsiasi operazione all'insaputa del legittimo proprietario, Anche il funzionamento stesso dei virus si è "affinato". Una volta assunto il controllo del PC infetto, il criminale di turno ha a disposizione un'interfaccia grafica che gli consente di controllare centinaia di computer contemporaneamente, utilizzando anche dei filtri che selezionano le macchine da usare in base ai più disparati criteri come, per esempio, la nazione in cui si trovano. È possibile, quindi, decidere di attivare tutti i computer controllati in Spagna per avviare una campagna di spam, o usare tutti i PC infetti che si trovano in Australia per lanciare un attacco contro un determinato sito Web.



Se il nostro PC è infetto, può essere usato per inviare email di spam o, ancora peggio, messaggi che cercano di attirare nuove vittime su siti di phishing.

PROTETTI MA NON INFETTI

La campagna lanciata da Panda Security si chiama Infected or not ed è stata avviata da uno studio che ha analizzato un milione e mezzo di computer già protetti da un antivirus. L'analisi è stata condotta usando un database che comprende 11 milioni di virus. I risultati sono sconfortanti: il 22,97% dei PC analizzati, infatti, erano infetti. La percentuale sale al 35% quando si tratta di computer che hanno un sistema di protezione non aggiornato. L'analisi riguardante le reti aziendali, poi, mostra dati ancora più preoccupanti: a essere infette sono il 72% delle reti. Il sistema di scansione ondine è disponibile per tutti all'indirizzo Internet www.infectedornot.com e richiede solo una breve procedura di registrazione.

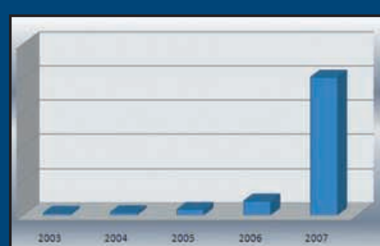


:: Al miglior offerente

La catena del crimine informatico, però, non si ferma qui. Difficilmente, infatti, chi gestisce una botnet rischia in prima persona. I pirati informatici di "seconda generazione" preferiscono infatti lavorare per altri, vendendo i loro servizi in siti specializzati. Dal sito si può prenotare l'invio di spam o anche un attacco contro il sito Internet di un'azienda concorrente.
Anche le informazioni riguardo i dati delle carte di credito che i pirati riescono a rubare non vengono utilizzati subito, ma rivenduti ad altre organizzazioni che si occupano di far fruttare l'investimento attraverso alcuni stratagemmi che gli garantiscono l'immunità. Si tratta di vere "società" specializzate, che reclutano via Internet degli ingenui disposti a eseguire delle "transazioni finanziarie".
In pratica, le persone assoldate a

CRESCITA ESPONENZIALE

Negli ultimi anni, i laboratori antivirus hanno registrato milioni di nuovi virus. L'aspetto più inquietante, però, è il tasso di crescita di nuove versioni: nel 2007, infatti, è stato rilevato un numero di nuovi virus superiore di 10 volte rispetto al 2006. A cambiare, però, è anche il tipo di virus. Crescono infatti i trojan, usati per controllare a distanza i PC e rubare informazioni. Nel 2005 rappresentavano solo il 49% del totale dei nuovi virus rilevati, nel 2006 il 63% e nel 2007 addirittura il 75%.





Navigando su Internet possiamo rintracciare decine di siti che offrono servizi legati all'uso di spyware e adware. Tutto avviene alla luce del sole.

questo scopo hanno il compito di aprire un conto corrente in una banca, ricevere somme di denaro, trattenere una minima percentuale della somma e inviare all'estero il rimanente. I paesi di destinazione, spesso situati nell'Europa dell'est, sono scelti secondo precisi criteri: sono tutte nazioni in cui qualsiasi indagine ha buone probabilità di finire in nulla.

L'operazione consente di "ripulire" il denaro, facendo in modo che i mediatori reclutati per ricevere e inviare il denaro siano gli unici che le forze dell'ordine possano rintracciare.

:: Carattere diverso

Ma come influisce tutto questo sul funzionamento degli antivirus? Questa diversa organizzazione ha stravolto anche gli obiettivi degli autori di malware. I virus di vecchia generazione erano programmati per garantire la massima visibilità: bloccavano il computer, visualizzavano messaggi minacciosi o spiritosi, provocavano malfunzionamenti che ne rendevano immediatamente visibile la presenza. Oggi, invece, un "buon" virus deve passare inosservato, installarsi senza danneggiare il computer e agire nell'ombra per far guadagnare denaro al suo creatore. Non a caso, il 75% dei virus comparsi nel 2007 sono trojan, una famiglia di virus che non ha la capacità di diffondersi autonomamente ma consente all'autore di controllare la macchina a distanza. I pirati informatici, però, hanno adottato anche altre strategie che hanno messo in crisi i laboratori antivirus, rendendo il loro lavoro estremamente difficile.

:: Il punto debole

I programmi antivirus usano diverse tecniche per individuare i programmi pericolosi. Le più evolute si basano sull'analisi delle operazioni compiute dai programmi, ma richiedono l'impiego di molte risorse e rallentano terribilmente il lavoro del computer. La tecnica più usata, quindi, rimane quella delle definizioni: il programma antivirus analizza il codice dei file e lo confronta con un database al cui interno sono memorizzati i virus conosciuti.
Il primo punto debole di questo sistema riguarda la creazione del database. Affinché un virus sia riconosciuto, infatti, è necessario che il laboratorio antivirus abbia ricevuto un "esemplare" del virus, chiamato in gergo sample. I sample arrivano da diverse fonti: dalle segnalazioni degli utenti che hanno installato l'antivirus, da altri laboratori di

NELLO SCHERMO DEI CRIMINALI

Una volta diffuso il virus, i pirati informatici possono controllare tutti i computer infetti da una singola postazione. Il sistema di controllo è tutt'altro che spartano: consente di suddividere i computer per nazionalità, inviare comandi specifici e visualizzare statistiche dettagliate riguardo l'attività di ogni gruppo di PC.



MPack v0.90 stats

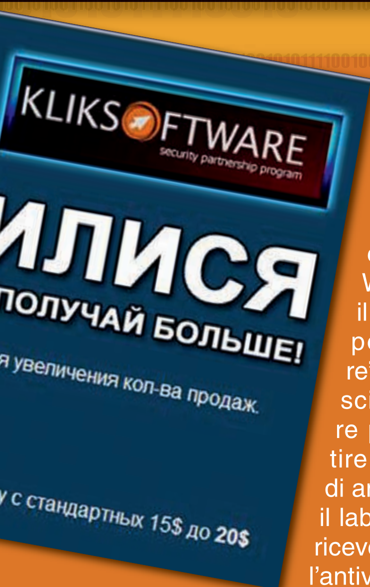
Attacked hosts (total - uniq)	
IE XP ALL	114721 - 96104
QuickTime	2175 - 2048
Win2000	7033 - 6260
Firefox	12885 - 12514
Opera7	1271 - 1264

Traffic (total - uniq)	
Total traff	159073 - 129089
Exploited	44804 - 35574
Loads count	17408 - 15968
Loader's response	38.85% - 44.89%
Efficiency 10.94% - 12.37%	

Browser stats (total)	
MSIE	4 0%
Opera	1 0%

Modules state	
Statistic type	MySQL-based
User blocking	ON
Country blocking	OFF

Country	Traff	Loads	Efficiency
RU - Russian federation	112793 70.9%	12653 72.7%	11.22%
UA - Ukraine	16666 10.5%	1670 9.6%	10.02%
IT - Italy	7045 4.4%	593 3.4%	8.42%
GE - Georgia	5775 3.6%	673 3.9%	11.65%
BY - Belarus	5419 3.4%	657 3.8%	12.12%
KZ - Kazakstan	3098 1.9%	376 2.2%	12.14%
US - United states	1117 0.7%	50 0.3%	4.48%
AZ - Azerbaijan	1060 0.7%	128 0.7%	12.08%
MD - Moldova, republic of	683	101	14.79%



sicurezza e dagli honey bot, computer che sono collegati al Web e hanno il preciso scopo di "attirare" i virus e lasciarsi infettare per consentire agli esperti di analizzarli. Se il laboratorio non riceve un sample, l'antivirus non sarà in grado di riconoscere il malware. Il secondo punto debole riguarda le dimensioni del database. Secondo un recente studio, sul Web circolano circa 11 milioni tra virus, trojan e spyware. Un archivio che li comprenda tutti sarebbe estremamente "ingombrante" e la comparazione impegnerebbe troppo il processore. Per questo motivo, i



Il sito www.infectedornot.com consente di analizzare il PC per verificare l'eventuale presenza di virus "nascosti".

IDENTIKIT

Spesso basta guardare una persona in faccia per capire che tipo sia. Nel caso dei pirati informatici, basta dare un'occhiata a queste foto di repertorio per capire come siano cambiate le cose. A sinistra vediamo gli autori di virus come Blaster, Sasser e NetSky. Si tratta di giovani programmatori che hanno agito per ottenere la fama o in alcuni casi per semplice incoscienza. A destra, invece, ci sono i ritratti di due pirati arrestati per phishing e spam nel corso degli ultimi mesi.







Alcune delle immagini catturate durante la "convention dei pirati russi", oltre ai virus sanno anche come far festa..



Per vendere i loro "servizi", i pirati informatici usano normali siti Web. Da qui è possibile prenotare l'invio di spam in uno specifico paese o richiedere un attacco Denial of Services contro un sito.

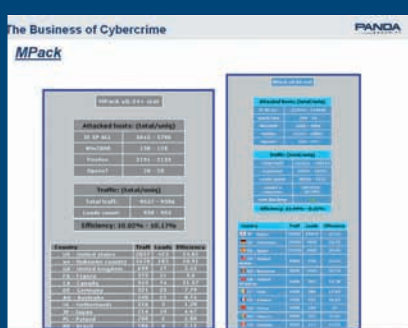
database degli antivirus in commercio comprendono solo i virus più pericolosi e diffusi, ma non ci garantiscono da quelli meno noti.
Infine, la maggior parte dei laboratori antivirus si affidano ancora a un'analisi "manuale" dei sample, che vengono studiati da esperti per valutarne l'eventuale pericolosità. Una sorta di processo "artigianale" che ha nel fattore tempo il suo più grande limite.

:: Fuori controllo

I pirati informatici hanno colpito proprio sfruttando queste debolezze, aumentando in maniera esponenziale il numero di varianti di ogni virus e riducendone la diffusione. In pratica, negli ultimi 18 mesi sono comparsi numerosi virus diversi, ognuno dei quali ha colpito solo qualche centinaio di computer. Tra le tecniche usate c'è anche l'uso di sistemi di compressione e crittografia che modificano radicalmente l'aspetto del codice mantenendo inalterate le funzioni. Una tecnica che mette in crisi i sistemi basati su definizioni. I cyber-criminali hanno così ottenuto un doppio scopo: da una parte hanno "intasato" i database dei laboratori antivirus, mentre dall'altro hanno ridotto le probabilità che i loro virus vengano individuati e analizzati. Secondo i dati di molti esperti, ogni giorno compaiono sul Web più di 15.000 nuovi sample, che è quasi impossibile classificare in tempo utile.

SENZA SPORCARSI LE MANI

Molti pirati non fanno nemmeno lo sforzo di controllare in prima persona quali informazioni sono riusciti a rubare. Si limitano a memorizzare i Log generati dai trojan, ovvero la registrazione di tutte le operazioni compiute dal PC infetto, rivendendole poi ad altri. Il sistema di pagamento è "a peso": 30 dollari per 50 MB di dati..



:: Le contromisure

Per contrastare questa offensiva, molte società antivirus stanno puntando a sviluppare sistemi alternativi, che consentano di rispondere con maggiore velocità ed efficacia all'ondata di virus che sta attraversando il Web. Le strategie, però, sono molto diverse. Molti laboratori, infatti, puntano a sistemi che analizzino le funzioni dei programmi, adottando un sistema che viene definito euristico. A distinguersi sono invece Sophos e Panda Security, che hanno entrambi

realizzato un sistema per l'analisi automatica dei sample, riducendo così l'intervento umano ai soli casi in cui il server che analizza i file abbia qualche "dubbio" sulla pericolosità del software.

:: Nuova soluzione

Automatizzare l'analisi dei file consente di offrire una risposta più rapida quando si riceve un sample, ma non migliora la situazione il loro reperimento.

La risposta di Panda Security a questo problema si chiama Intelligenza collettiva e, almeno sulla carta, è molto interessante. L'antivirus, in pratica, attiva una particolare procedura ogni volta che sulla macchina "compare" un nuovo processo. L'analisi del processo all'interno del PC, però, non è particolarmente approfondita: viene invece richiesta via Internet a un gruppo di server specializzati, che analizzano il programma per stabilire se si tratti di un virus o meno. Le informazioni così ottenute vengono memorizzate e vanno a formare una sorta di "database remoto". Quando un altro computer con antivirus Panda segnalerà la comparsa dello stesso processo, la risposta arriverà quindi in un attimo. Grazie a questa tecnica, l'Intelligenza collettiva dovrebbe essere in grado di individuare anche i virus meno diffusi, andando così a coprire una "zona grigia" che oggi consente ai pirati informatici di agire impunemente.

QUANTO GUADAGNANO?

Le attività dei pirati informatici di nuova generazione sono estremamente lucrose. In uno dei casi recentemente analizzati dagli esperti di sicurezza, l'organizzazione individuata era in grado di controllare più di 70.000 computer infetti. Calcolando i guadagni stato per stato, si arriva a un totale di circa 850.000 dollari al mese.



In molti casi, le attività dei pirati sono tutt'altro che clandestine: questa foto in cui viene mostrato il frutto dell'attività di spam è stata tranquillamente pubblicata sul sito ufficiale della società

:: La battaglia continua

Per verificare la validità di un sistema come l'Intelligenza collettiva sviluppato da Panda Security, è necessario un po' di tempo ed è probabile che in caso di successo altri produttori di antivirus seguiranno una strada simile. Resta da vedere quali saranno le contromosse dei pirati informatici, che potrebbero per esempio puntare su un potenziamento dei rootkit, ovvero quei programmi che hanno la capacità di "nascondere" un processo al sistema operativo. La partita, quindi, è ancora aperta. ■

IL MERCATO NERO

Ecco un elenco con i prezzi medi pagati per l'acquisto di informazioni rubate tramite trojan. Tra i "beni" disponibili ci sono anche gli account di popolari videogiochi ondine come World of Warcraft, venduti a prezzi da brivido, e anche quelli del popolare programma messenger ICQ. Sul Web, infatti, gli account con numeri "bassi" di ICQ, ovvero quelli a 6 o 7 cifre, sono considerati "pregiati".

- Account FTP	1 dollaro
- Account ICQ	Tra 1 e 10 dollari
- Account di un negozio online (solo russi)	50 dollari
- Carte di credito VISA o Mastercard	da 1,50 a 2 dollari
- Passaporti in bianco e nero	2 dollari
- Passaporti a colori	5 dollari



DISCOGRAFICI Vs P2P



La nuova sfida, fra tutela della privacy e diritto d'autore

Negli ultimi mesi si è rinfocolata l'annosa polemica fra chi ritene ammissibile utilizzare la Rete per scaricare materiale protetto da copyright e chi, invece, desidera proteggere gli interessi di coloro i quali realizzano opere per la cui fruizione è normalmente previsto il pagamento di un corrispettivo in denaro.

In gioco, come al solito, c'è molto altro. La Rete, per continuare ad essere Agorà della controcultura, dell'informazione altrimenti non fornita, della libera ricerca, dovrebbe essere tenuta al riparo da ogni possibile vincolo, tuttavia, perché i diritti di chi vive sul commercio delle proprie opere vengano rispettati, sembra ad alcuni necessario introdurre "legalmente e istituzionalmente" nuovi vincoli. Nel problema concreto si cela quindi un'importante questione di principio. Un precedente, qualcosa che potrebbe modificare radicalmente Internet mutandone la sua stessa essenza. Per chiarirci le idee abbiamo intervistato l'Avvocato Marco Pierani, Responsabile relazioni istituzionali per Altroconsumo.

1) Negli ultimi tempi appare sempre più evidente una strategia di accerchiamento da parte dei discografici nei confronti dei provider internet, come la descrive?

Il tentativo, che è in atto in tutta Europa e non solo in Italia, rappresenta un nuovo e preoccupante tassello di quella peculiare escalation che ha avuto negli ultimi anni la lotta senza quartiere alla così detta "pirateria" nella quale sono da tempo impegnate le major dell'audiovisivo. In sostanza la novità sta nel fatto che si sta cercando di rendere più "organici" i provider nell'enforcement della proprietà intellettuale introducendo forme di filtraggio dei contenuti digitali alla fonte e la possibilità che, a seguito di un primo "avvertimento" per pretese violazioni del diritto d'autore, i providers decidano unilateralmente di privare all'utente l'accesso alla Rete. Questo



L'homepage del sito di Altroconsumo: www.altroconsumo.it

è già previsto in Francia dall'accordo raggiunto sulla base dei lavori della Commissione Olivennes, mentre in Inghilterra è oggetto di un'apposita proposta di legge.

2) Molti sostengono che il mercato discografico si stia contraendo a causa della pirateria on-line. Ritiene che ciò sia vero?

È fuori di dubbio che esista una sorta di "mercato parallelo", quello del p2p dove milioni di persone scambiano contenuti ledendo più o meno coscientemente il diritto d'autore, tuttavia appare innegabile che lo sviluppo di tale fenomeno è dovuto in larga parte proprio alla originaria ritrosia delle major ad utilizzare Internet quale nuovo canale di distribuzione. Insomma, colpite da un classico esempio di disruptive technology le major hanno per lunghi anni protetto in tutti i modi il oro obsoleto modello di business e solo ora cominciano seriamente a guardare all'on-line, nel frattempo però visto che c'era domanda e c'era la tecnologia i contenuti sono comunque stati distribuiti ma illegalmente, verrebbe da dire chi è causa del suo mal pianga se stesso!

3) Come secondo lei dovrebbe evolvere il modello di commercio degli audiovisivi nell'era di Internet?

È importante che non si persegua la strada dei walled garden e delle artificiali segmentazioni verticali. Penso che nel futuro potranno coesistere vari modelli che si confronteranno tra loro, ma il substrato tecnologico di base sul quale opereranno sarà ancora il DRM. So bene che le forme proprietarie di DRM che abbiamo conosciuto fino ad ora evocano esperienze assolutamente negative, ma non è tempo di fare la caccia alle streghe, anche i consumatori con responsabilità debbono essere propositivi e allora un modello di DRM interoperabile, che non sia più quello strumento di protezione coattiva dei diritti unilateralmente imposto che abbiamo conosciuto ma, al contrario, uno strumento di traduzione tecnologica di un nuovo assetto negoziale concordato tra consumatori e distributori di prodotti culturali, appare percorribile. D'altra parte il diritto d'autore nella società dell'informazione non potrà certo fare a meno di un supporto tecnologico.

4) Stante l'attuale ordinamento legale della nostra nazione, quale sono i rischi concreti per i navigatori italiani che scaricano illegalmente attraverso le reti peer-to-peer materiale coperto da copyright?

Quali sono le differenze in tal senso fra chi fruisce di simili contenuti a titolo personale e chi, invece, ne fa commercio?

Attualmente il semplice downloader rischia sanzioni esclusivamente amministrative, in particolare quelle previste dall'art. 174-ter l.d.a. (154 Euro aumentati fino a 1032 Euro in caso di recidiva o di fatto grave per la quantità delle violazioni). Ma, com'è noto, è alquanto improbabile, per come sono strutturati la maggior parte dei sistemi peer-to-peer che un downloader non sia nella pratica anche uploader. Il soggetto che, invece, senza una contropartita economica, condivide o, comunque, utilizza anche quale mero downloader una piattaforma peer-to-peer che per motivi tecnici di funzionamento prevede di default la messa in condivisione automatica di quanto scaricato, rischia già la sanzione penale di cui all'art. 171 comma 1 lettera a-bis l.d.a., una multa da Euro 51 a Euro 2.065. Chi, infine, condivide a fini di lucro, rischia la reclusione da uno a quattro anni nonché una multa fino a oltre 15.000 Euro ai sensi dell'art. 171-ter, comma 2, lett. a-bis.

5) Quali sono, secondo lei, i rischi per le libertà e per la privacy dei fruitori italiani della Rete qualora le istanze dei discografici dovessero essere accolte?

Come dicevo prima, fare degli ISP una sorta di gendarmi della Rete sarebbe sbagliato e stiamo facendo di tutto perché questo non avvenga. Se questa sarà la strada che verrà intrapresa, l'applicazione di tecniche di filtraggio massiccio potrebbe avere gravi conseguenze sulla libertà di espressione e di pensiero, allo stesso modo l'investigazione privata da parte dei titolari dei diritti coadiuvati dagli ISP significherebbe lo snaturamento dei principi del diritto penale e, più in generale, una sconfitta per la certezza del diritto.

6) Di recente il Garante della Privacy si è occupato più volte della questione, cosa ha smosso le acque rendendo la pirateria audiovisiva sulla Rete un argomento tanto "caldo"?

È stato il caso Peppermint, in sostanza attraverso un apposito software della Logistep (società svizzera) una piccola casa discografica tedesca, la Peppermint appunto, ha individuato gli indirizzi IP di moltissimi italiani che utilizzavano reti p2p e che avrebbero condiviso titoli della Peppermint ledendo i suoi diritti. Successivamente, attraverso un avvocato di Bolzano, la Peppermint ha promosso alcuni procedimenti civili d'urgenza presso il Tribunale di Roma perché quest'ultimo ordinasse agli ISP di fornire nomi e indirizzi fisici da abbinare agli indirizzi IP.

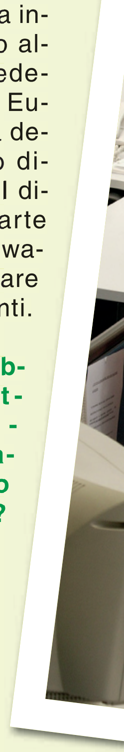
7) Potrebbe descrivere l'attuale orientamento del Garante della Privacy in proposito?

Dopo che il Tribunale di Roma ha ordinato in due prime occasioni agli ISP di fornire i dati, il Garante per la Privacy è intervenuto nei successivi procedimenti civili d'urgenza e il Giudice, accogliendo le istanze proposte dal Garante, ha rigettato i ricorsi con i quali la Peppermint chiedeva di ottenere ulteriori nomi di migliaia di utenti di reti p2p proprio perché operando un bilanciamento tra la tutela del diritto d'autore e la tutela della privacy ha deciso che a prevalere doveva essere la seconda.

Giova anche ricordare che Altroconsumo ha promosso presso lo stesso Garante Privacy un maxireclamo in favore di circa 100 consumatori raggiunti dalla fatidica raccomandata intimatoria con la quale l'avvocato altoatesino della Peppermint chiedeva un risarcimento di oltre 300 Euro ed il Garante recentemente ha deciso in favore di Altroconsumo dichiarando illegittimo e lesivo del diritto alla privacy l'utilizzo da parte della Peppermint stessa del software della Logistep per rilevare gli indirizzi IP degli utenti.

8) Cosa dobbiamo attenderci dal futuro, quali saranno, secondo lei, le evoluzioni?

La posizione presa dal Garante Privacy nel caso Peppermint è importante anche perché di poco successiva alla sentenza della Corte di Giustizia europea nell'analogo caso Promusicae con la quale, in sostanza, il Giudice Europeo invitava ogni singolo Stato membro a individuare nel proprio ordinamento un equo bilanciamento tra la tutela del diritto d'autore e la tutela della privacy.
Dopo la decisione del Garante nel caso Peppermint, dunque, appare possibile affermare che anche l'Italia si allinea ad altri esempi positivi come quelli della Germania e della Spagna dove gli ISP possono essere costretti a rivelare i dati personali soltanto in procedimenti penali.



9) Ritiene che qualche fruitore di file scaricati illegalmente possa ricevere anche oggi richieste di risarcimento?



Foto della direzione e dello staff di Altroconsumo
Credits: A. Roveri

Ritengo che un comportamento come quello dell'avvocato altoatesino non avrà a ripetersi anche perché censurabile dal punto di vista deontologico. La situazione è comunque in divenire e indubbiamente i titolari dei diritti possono intraprendere altre forme e modalità di tutela. Rimane il fatto che scaricare o condividere file protetti da diritto d'autore può configurare, come si è detto, anche ipotesi di reato. Vorrei in conclusione affermare con chiarezza che riteniamo giusto e corretto che la proprietà intellettuale sia tutelata ma questo non può e non deve comportare un vero e proprio calpestamento dei diritti degli utenti.

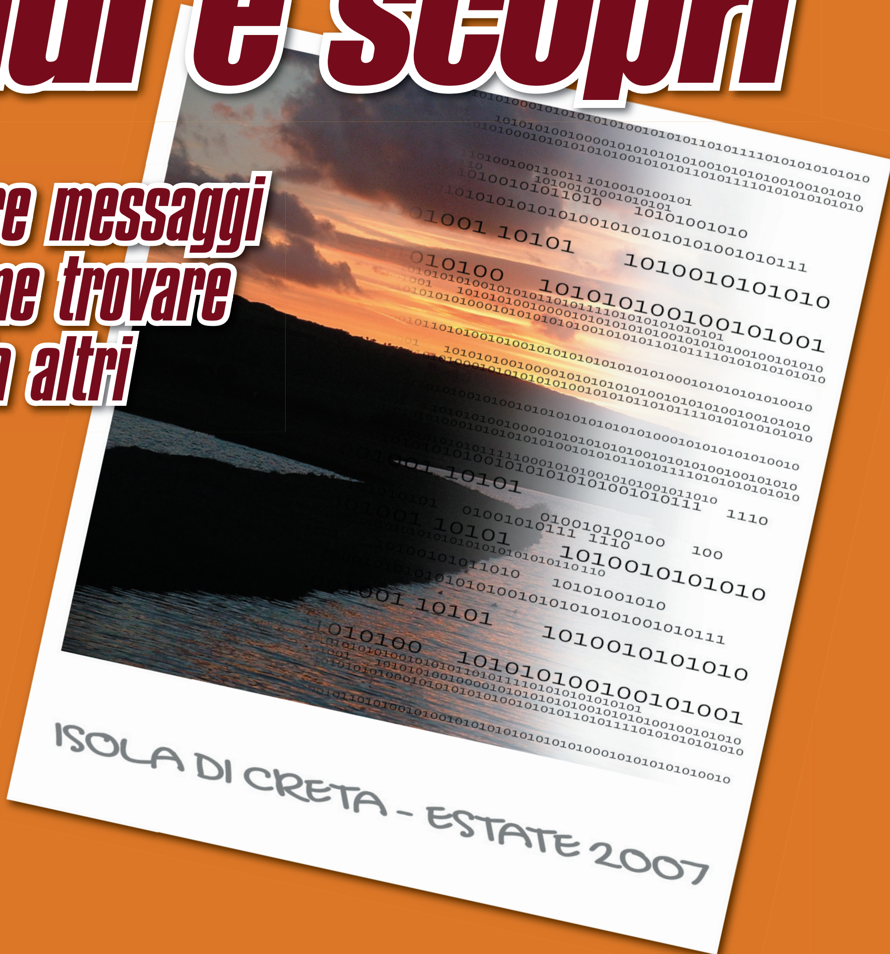
Francesco Principe

CHI SONO?

Altroconsumo è un'associazione di consumatori che con i suoi 300.000 Soci e i suoi 30 anni di attività può essere considerata la prima e la più importante in Italia. Indipendente e senza fini di lucro, ha come unico obiettivo l'informazione e la tutela dei consumatori. La tutela degli interessi e i diritti fondamentali dei cittadini si esprime in tutti i settori: la protezione della salute e della sicurezza, la tutela degli interessi economici, il diritto a essere informati, a conoscere i propri diritti e a far valere le proprie ragioni, il diritto a essere rappresentati e ascoltati presso le istituzioni nazionali e internazionali, il diritto a vivere in un ambiente sano e a compiere scelte di consumo etiche e responsabili.
Per informazioni: www.altroconsumo.it

STEGANOGRAFIA: nascondi e scopri

Scopriamo come creare messaggi nascosti nei file e come trovare i messaggi nascosti da altri



Nascondere delle informazioni in altre informazioni, senza che queste ultime sembrino esser state modificate: ecco il significato della parola steganografia. Per un esempio pratico, pensiamo alla possibilità di poter inviare dei dati sensibili (un recapito telefonico, un indirizzo che vogliamo tenere nascosto, ecc...) per email ad una persona fidata, inserendoli in una serie di immagini. I dati arriveranno a destinazione, non destando alcun sospetto in altri eventuali lettori, magari accidentali, della nostra posta. Andiamo a scoprire, dunque, alcuni software di steganografia per Linux.



Sembra una comune immagine delle vacanze, eh? Invece contiene una manciata di segretissimi numeri di telefono!

:: Nascondiamo con outguess

Il programma più importante, chiaramente, è quello che ci servirà per poter nascondere le informazioni. Installeremo outguess. Scarichiamolo dal sito entrando nella sezione Download. Una volta che abbiamo prelevato l'archivio dei sorgenti (outguess-0.2.tar.gz), scompattiamolo (tar xvfz outguess-0.2.tar.gz) ed entriamo nella directory appena creata; a questo punto per compilare outguess eseguiamo in "./configure" e, quindi, "make". Per installare nel sistema i binari compilati diventiamo root con "su -" (o "sudo -s" se usiamo Ubuntu) e lanciamo il comando

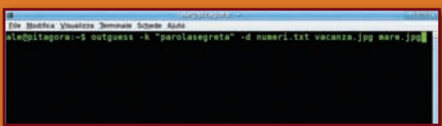
```
"make install".
```

L'utilizzo di outguess è davvero semplice. Innanzitutto, bisogna dare in pasto al programma un'immagine in formato JPEG, PPM o PNM, quindi un'immagine finale che conterrà anche le informazioni nascoste; poi viene richiesta una chiave, che servirà a crittare e decrittare le informazioni che andremo ad inserire nell'immagine, ed infine bisogna indicare al programma il file di

testo contenente le informazioni da aggiungere.

:: Un esempio pratico

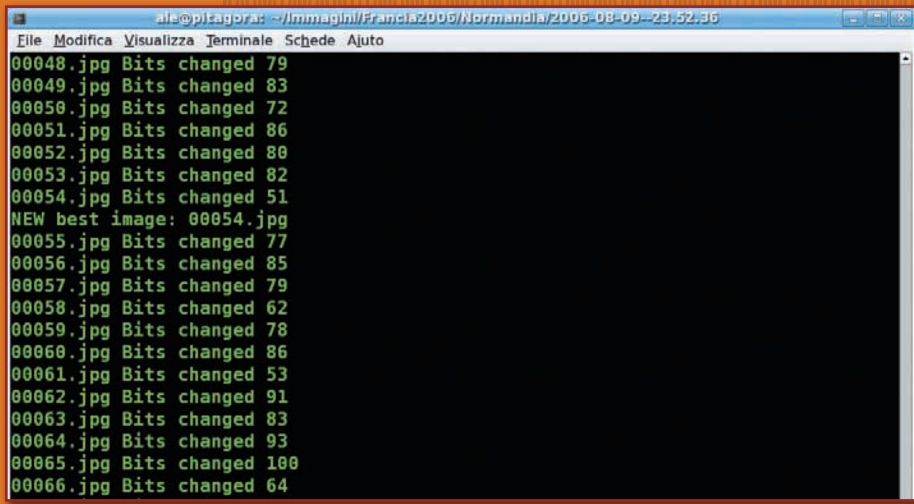
Vediamo come nascondere il testo contenuto nel file numeri.txt (che possiamo creare con un qualsiasi editor) all'interno dell'immagine vacanza.jpg. In console lanciamo 'outguess -k "parolasegreta" -d numeri.txt vacanza.jpg mare.jpg'. Il parametro "-k" contiene la chiave di crittazione, "-d" il testo da nascondere mentre mare.jpg è l'immagine finale.
La persona a cui invieremo l'immagine mare.jpg per leggere il messaggio nascosto non dovrà fare altro che eseguire 'outguess -k "parolasegreta" -r mare.jpg messaggio.txt': il contenuto di messaggio.txt sarà proprio il messaggio nascosto.



La sintassi di outguess per inserire un messaggio nascosto in un'immagine.

:: Scegliamo l'immagine migliore

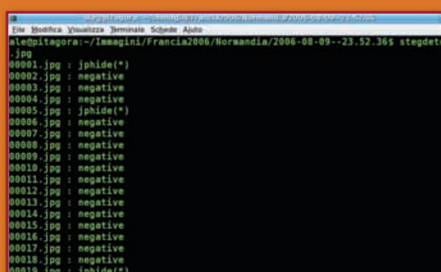
L'inserimento di informazioni in un file produce, comunque, dei cambiamenti nel file stesso: è importante che tali cambiamenti siano meno invasibili possibile. Nel pacchetto dei sorgenti di outguess è incluso uno script chiamato seek_script; questo ricerca nella directory corrente l'immagine che necessita del minor numero di alterazioni per inglobare il messaggio che vogliamo celare.
Per richiamare lo script, dunque, apriamo una console ed entriamo in una directory piena di immagini JPEG. Con un editor scriviamo il messaggio da nascondere nel file /tmp/fortune; quindi lanciamo semplicemente "seek_script". Lette tutte le immagini nella directory, avremo in output una riga del tipo "Best data object was 00001.jpg with 361. Worst result was 390.": la migliore immagine da usare per nascondere il messaggio, in questo esempio, è perciò 00001.jpg.



Scopriamo quale immagine è la più adatta per contenere il nostro messaggio nascosto.

:: Snidiamo le informazioni nascoste

A volte può essere istruttivo (o, perché no, divertente) scoprire se in un'immagine è presente un'informazione nascosta tramite steganografia. Per fare questo possiamo far uso di stegdetect, che effettua dei test statistici su immagini JPEG per individuare quelle che sono state alterate da software di steganografia come jsteg, jphide ed il nostro outguess (ma la versione 01.3b, non quella attuale).
Scarichiamo stegdetect dal sito di Outguess e seguiamo la consueta procedura per la compilazione e l'installazione ("./configure", "make", "make install"). Attenzione, il programma non si compila con GCC-4.1, quindi è necessario passare momentaneamente a GCC-3.4; se usiamo la distro Ubuntu, quindi, cancelliamo il link simbolico /usr/bin/gcc ("rm /usr/bin/gcc") e creiamone uno nuovo con "ln -s /usr/bin/gcc-3.4 /usr/bin/gcc", quindi effettuiamo la compilazione.



Ci sono immagini con contenuti nascosti? Scopriamolo con stegdetect...

Per usare stegdetect entriamo in una directory piena di immagini e lanciamo "stegdetect *.jpg". In output ci verranno segnalate con degli asterischi le immagini probabilmente manipolate da programmi di steganografia: un numero maggiore di asterischi indica una probabilità maggiore di contenere informazioni nascoste.

:: Decifriamo il messaggio nascosto

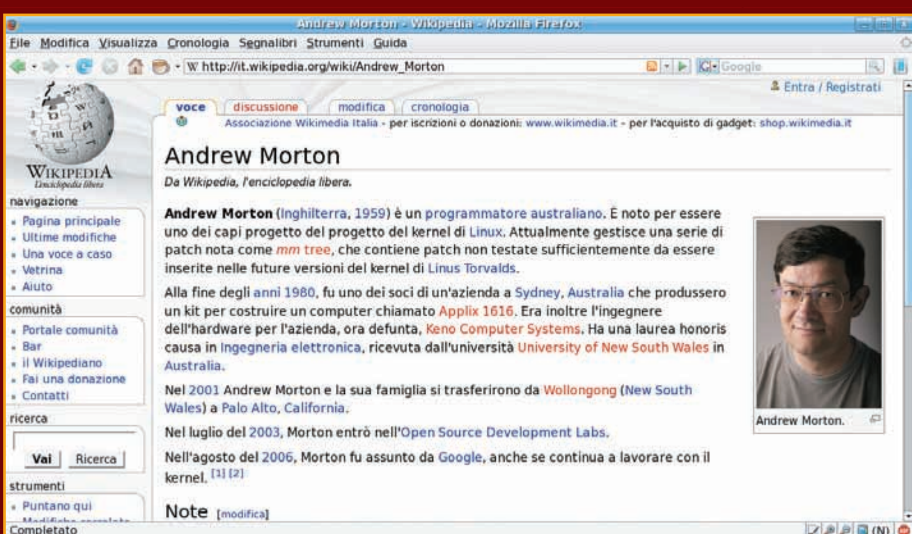
Una volta individuata l'immagine contenente un messaggio nascosto, possiamo usare stegbreak (contenuto nei sorgenti di stegdetect) per trovare la chiave di crittazione utilizzata mediante un attacco a forza bruta. Installiamo nel sistema un file dizionario per effettuare l'attacco (ad esempio, il pacchetto wbritish su Ubuntu), quindi lanciamo stegbreak in questo modo: "stegbreak -tj immagine.jpg". Il parametro '-t' è seguito da una lettera che indica il programma di steganografia che, secondo stegdetect, è stato usato per manipolare l'immagine (man stegbreak per maggiori informazioni). Se il dizionario per l'attacco non è nella posizione standard /usr/share/dict/words, indichiamo il path corretto tramite l'opzione -f ("-f /usr/local/dict/words", ad esempio).
Ottenuta la chiave di cifratura, non ci resterà che usare outguess per decifrare il messaggio nascosto nell'immagine. ■

Pimp my Penguin

Installiamo l'ultima versione del kernel ed applichiamo le patch di Andrew Morton



Il kernel fornito dalle più diffuse distribuzioni è un kernel solitamente molto testato, affidabile e solido. Oltre che, altrettanto solitamente, piuttosto recente. A volte, però, sentiamo il bisogno di sperimentare: provare nuove funzionalità, magari un poco rischiose, scoprire se il driver per un nostro dispositivo è stato migliorato oppure, semplicemente, seguire passo dopo passo gli sviluppi del centro nevralgico del sistema operativo. Tutto nel più puro spirito dell'hacker.



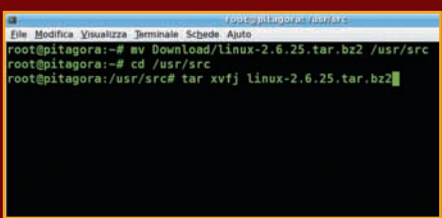
In queste due pagine, quindi, scopriremo... il lato intrepido del kernel: scaricheremo l'ultima versione del kernel, applicheremo le patch sperimentali "-mm" di Andrew Morton e compileremo poi il tutto. Il risultato sarà un nuovo kernel da lanciare all'avvio del PC, ricco di novità e probabilmente più performante di quello di default.

:: Scarichiamo l'ultimo kernel

Iniziamo dal download dei sorgenti ufficiali del kernel: per applicare le patch "-mm", infatti, è

◄ *Questo articolo è sotto il segno di Andrew Morton, l'autore delle patch che andremo ad applicare al kernel.*

necessario disporre di questi, mentre i sorgenti modificati dalle singole distro spesso non consentono di portare a compimento l'operazione. Puntiamo il nostro web browser all'indirizzo http://www.it.kernel.org/pub/linux/kernel/v2.6/ e scarichiamo l'ultima release del kernel, attualmente la 2.6.25 (il file da prelevare sarà quindi linux-2.6.25.tar.bz2).
Apriamo una console. Per comodità, per lanciare i comandi indicati nel corso dell'articolo assumiamo immediatamente i poteri di root con "su --login" oppure con "sudo -s" (quest'ultimo comando se usiamo Ubuntu). Spostiamo l'archivio appena scaricato in /usr/src: entriamo nella directory in cui Firefox salva i download e digitiamo "mv linux-2.6.25.tar.bz2 /usr/src". A questo punto entriamo in /usr/src con "cd /usr/src" e scompattiamo l'archivio con "tar xvfj linux-2.6.25.tar.bz2".



Scarichiamo, scompattiamo e spostiamo i sorgenti del kernel.

:: Scarichiamo le patch

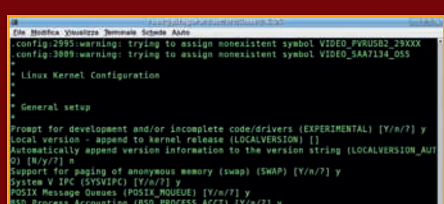
Le cosiddette patch "-mm" costituiscono una sorta di serbatoio per le sperimentazioni: qui confluiscono funzionalità innovative e driver aggiornati, prima di venire testati con accuratezza ed esser poi disciplinatamente incanalati nel ramo stabile del kernel. Insomma, queste patch sono una specie di "giornale del giorno dopo": il sogno di ogni hacker che si rispetti, anche a rischio di un poco di stabilità di sistema in meno...
È necessario scaricare il file delle patch che corrisponda esattamente alla release del kernel sulla quale vogliamo applicarle. Apriamo dunque con il browser la pagina http://www.kernel.org/pub/linux/kernel/people/akpm/patches/2.6/ ed entriamo nella cartella 2.6.25, poi nella directory 2.6.25-mm1. Qui preleviamo finalmente il file delle patch, 2.6.25-mm1.bz2.

:: Applichiamo le patch

Arrivati a questo punto, non dobbiamo far altro che applicare le patch al kernel. Copiamo il file 2.6.25-mm1.bz2 nella directory /usr/src, entriamo nella cartella in cui sono stati scompattati i sorgenti del kernel ("cd /usr/src/linux-2.6.25") e, quindi, applichiamo le patch lanciando "bzcat ../2.6.25-mm1.bz2 | patch -p1". Diamo le ultime rifiniture creando un link alla directory del kernel: "ln -s /usr/src/linux-2.6.25 /usr/src/linux". Ora possiamo passare alla compilazione del nuovo kernel.

:: La configurazione? Quella vecchia!

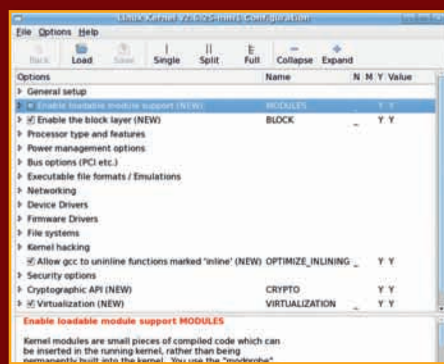
Prima di compilare il kernel, per semplificarne la configurazione si consiglia di partire dalle opzioni attive nel kernel della nostra distribuzione. Faremo un travaso, insomma, dalla configurazione del kernel di default alla configurazione di quello che stiamo per compilare. Individuiamo il file di configurazione del kernel della distro: in Ubuntu Gutsy Gibbon, ad esempio, si tratta del file /boot/config-2.6.22-14-generic; copiamo questo file nella directory del kernel (che, nella console, è quella corrente) con "cp /boot/config-2.6.22-14-generic .config". Per importare la vecchia configurazione, quindi, lanciamo "make oldconfig". Ci verrà chiesto di configurare le opzioni del nuovo kernel che non erano presenti nel kernel di default: accettiamo i valori di default schiacciando Invio finché non veniamo riportati al prompt dei comandi.



Importiamo la configurazione del kernel fornita dalla nostra distro.

:: Il giusto ritocco alle opzioni

Adesso rivediamo l'intera configurazione del kernel, modificando se vogliamo i valori impostati nella configurazione della distro ed abilitando tutte le funzionalità che desideriamo. Per fare questo lanciamo in console "make gconfig" se usiamo Gnome o XFCE, "make xconfig" se siamo utenti KDE e, infine, "make menuconfig" se preferiamo configurare il kernel direttamente dal terminale; in tutti e tre i casi, comunque, avremo a che fare con una semplice ma efficace interfaccia.



Chi ha detto che per configurare il kernel non si possa usare una comoda interfaccia grafica? Ecco l'interfaccia di make gconfig.

:: Andiamo a compilare...

I comandi generici per compilare un kernel sono riassumibili in questa riga da eseguire in console: "make dep clean bzImage modules modules_install"; lanciamola ed attendiamo pazientemente che il kernel venga compilato ed installato nel sistema. Alcune distribuzioni, però, forniscono degli strumenti per automatizzare le procedure di compilazione, installazione e manutenzione di un kernel. Debian e derivate (come Ubuntu), ad esempio, permettono di compilare un kernel e creare un pacchetto apposito mediante un unico comando: in questo caso basta lanciare "make-kpkg --initrd kernel_image" (il comando make-kpkg si trova nel pacchetto kernel-package); al termine dell'esecuzione, troveremo in /usr/src un pacchetto .deb del kernel con le patch da noi applicate. Per installarlo ci basterà lanciare "dpkg -i pacchetto_kernel.deb". ■

KEYLOGGER

Come un Grande Fratello, i keylogger registrano ogni tasto che premiamo e lo inviano ai malintenzionati. Vediamo bene cosa sono...

Un keylogger è un semplice programma che rileva e registra i tasti premuti sulla tastiera di un computer. Solitamente non dà segni della sua presenza e intercetta tutti i comandi dati alle applicazioni inviati mediante tastiera. Le pressioni dei tasti così rilevate vengono registrate in un file.

A quel punto, il keylogger trasmette le informazioni a un hacker o attende che l'hacker si colleghi al computer infetto e recuperi il file registrato.

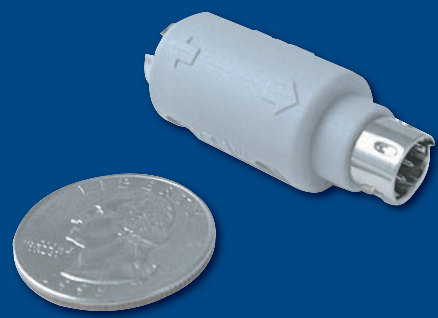
:: Non una backdoor ma pericoloso...

I keylogger non registrano ciò che i dati inseriti fanno visualizzare a schermo ma rilevano qualsiasi dato inserito in qualsiasi applicazione.

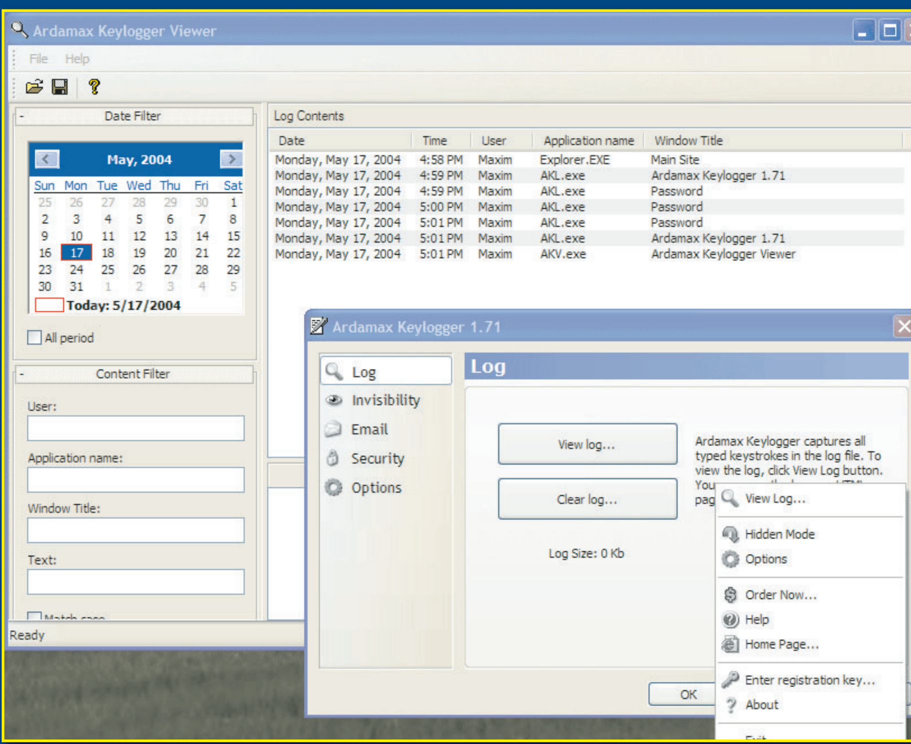
Per questo sono utili agli hacker per impadronirsi di nomi utente, password e altri dati importanti.

Dato che si tratta di informazioni vitali, è opportuno assicurarsi di essere in grado di rilevare ed eliminare i keylogger.

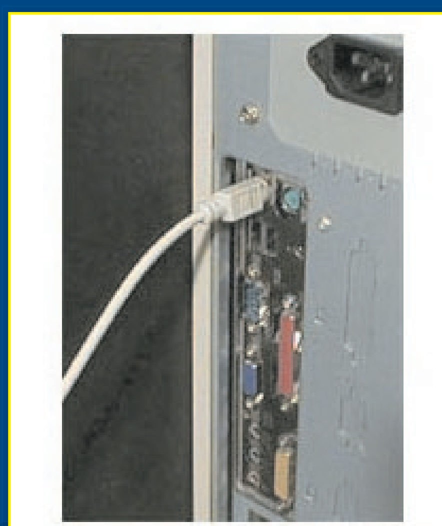
Un keylogger però può anche essere un dispositivo fisico vero e proprio: ci sono dei cilindretti che si applicano alla porta della tastiera sul computer e che registrano tutto ciò che viene digitato.



Ecco un keylogger "fisico" si inserisce fra il computer e la tastiera.



Un programma keylogger genera un semplicissimo log: consultiamolo e sapremo tutto quello che ha digitato l'utente dal computer infetto...



BACKDOOR

Immaginiamo di comprare gioielli e beni preziosi, di raccogliere tutti i nostri averi più cari e dopo averli messi in ordine in casa di consegnare la chiave delle porta a un ladro. Ecco cos'è una backdoor...

Una backdoor (letteralmente porta sul retro) in un computer è un metodo usato per saltare la normale autenticazione o per ottenere accesso remoto a un computer, senza essere identificati nel caso di un controllo. La backdoor può assumere la forma di un programma installato (come Back Orifice o come le backdoor che sfruttano illecitamente il sistema di Sony/BMG, che veniva installata ogni qual volta uno dei milioni di CD musicali Sony veniva riprodotto su un computer Windows) o di una versione modificata di un programma legittimo.

:: Backdoor anche al cinema

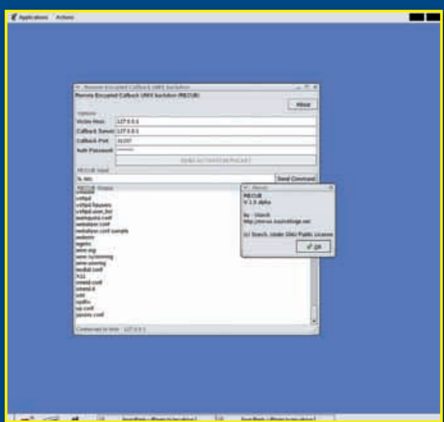
Una backdoor può essere tanto semplice quanto una combinazione utente-password preinserita nel sistema e che dà pieno accesso: inseriti questi dati si può accedere al computer, anche senza conoscere nome utente e password scelti dal proprietario. Un celebre esempio di backdoor di questo tipo compare nel film del 1983 War Games, in cui il creatore del sistema di computer "WOPR" aveva inserito una password segreta (il nome del figlio morto) che dava all'utente l'accesso al sistema e a parti segrete del computer. Sebbene il numero delle backdoor presenti in sistemi che usano programmi proprietari (cioè il cui codice sorgente non è direttamente esaminabile) non sia di dominio pubblico, vengono periodicamente (e frequentemente) scoperte. Alcuni programmatori sono riusciti perfino a installare segretamente grandi quantità di codici non dannosi (le cosiddette uova di Pasqua o Easter Egg) in alcuni programmi, sebbene in questi casi essi abbiano beneficiato del tacito accordo, se non dell'esplicita autorizzazione, da parte dell'azienda.

È possibile creare una backdoor anche senza modificare il codice sorgente di un programma, o perfino modificare quest'ultimo dopo la sua compilazione. È possibile fare questo riscrivendo il compilatore in modo che riconosca durante la compilazione il codice che innesca l'inserimento di una backdoor. Quando il compilatore truccato individua il codice, continua a operare normalmente ma inserisce anche una backdoor (per esempio una routine di riconoscimento password). In questo modo, quando l'utente inserisce il dato richiesto, ottiene l'accesso a parti (presumibilmente riservate) del funzionamento del programma.

:: Backdoor su commissione

Molti worm, come Sobig e Mydoom, installano una backdoor nel computer contagiato (generalmente un PC con connessione a banda larga che usa versioni non sicure di Microsoft Windows e Microsoft Outlook). Queste backdoor vengono installate apparentemente per consentire ai distributori di spam di inviare e-mail spazzatura dai computer infetti.

Altre backdoor, come quella che sfrutta il sistema che Sony/BMG distribuiva segretamente su milioni di CD musicali alla fine del 2005, agiscono addirittura sotto copertura, poiché il programma di Sony segretamente contattava regolarmente dei server centrali per inviare informazioni sull'uso della musica regolarmente acquistata. La backdoor tradizionale è di tipo cosiddetto simmetrico: chiunque la trovi può usarla.



Una backdoor può permettere un accesso al computer davvero sofisticato. Può mettere per esempio a disposizione del pirata una schermata in cui vede tutto quello che succede sul nostro monitor, con la possibilità ovviamente di prendere il controllo del sistema in qualsiasi momento.

Una backdoor asimmetrica può essere invece usata esclusivamente dall'aggressore che la installa, anche nel caso in cui venga scoperta e diffusa in pubblico. Per esempio, una backdoor può essere configurata in modo tale da permettere l'accesso da un solo computer.

I PANTALONI GEEK

Chi di noi non ha sognato di avere sempre con se la propria tastiera, il proprio mouse e le casse??? Beh!!! Da oggi potrete indossarle!!! Tutto grazie al designer Erik De Nijs che ha inventato questo straordinario paio di pantaloni full optional con tanto di tastiera, mouse e casse incorporate... Il top per ogni malato di informatica...









QUATTORD. ANNO 8- N°151- 15/28 MAGGIO 2008 - € 2,00